تجربة ديوان المحاسبة الكويتي بخصوص التشغيل الإلكتروني للبيانات وكيفية كتشاف وسائل الغش ومواطن الفساد

ديوان المحاسبة
State Audit Bureau
Since 1964 تأسس عام - الكويت Kuwait

نبذة عن ديوان المحاسبة
في الكويت

نشأة ديوان المحاسبة في دولة الكويت

- صدر دستور دولة الكويت في 11 نوفمبر سنة 1962، وقد نص بالنص صراحة على إنشاء ديوان للمراقبة المالية يكفل القانون استقلاله، إيماناً بأن المال العام هو عصب الدولة وعماد نهضتها ومن ثم يجب أن يحاط بسياج من الحماية لضمان جبايته كاملاً دون نقص أو تقصير وإنفاقه فيما يدعم المجتمع ويعود عليه بالنفع دون إسراف أو تقصير.

- في 7 يوليو سنة 1964 صدر القانون رقم 30 لسنة 1964 بإنشاء ديوان المحاسبة بدولة الكويت.

أهداف وأساليب الرقابة في ديوان المحاسبة

- تحقيق رقابة فعالة على الأموال العامة لصونها ومنع العبث بها والتأكد من استخدامها الاستخدام الأمثل في الأغراض التي خصصت لها.

- الأساليب الرقابية التي يتبعها ديوان المحاسبة لتحقيق أهدافه:

- رقابة مسبقة
- رقابة لاحقة
- رقابة أداء

الجهات المشمولة برقابة ديوان المحاسبة

تشـمل الرقابة التي يختص بها الديوان ، الجهات الآتية :

أولا : كافة الوزارات والإدارات والمصالح العامة التي يتألف منها الجهاز الإداري للدولة .

ثانيا : البلديات وسائر الهيئات المحلية ذات الشخصية المعنوية العامة .

ثالثا : الهيئات والمؤسسات والمنشآت العامة التابعة للدولة أو للبلديات أو لغيرها من الهيئات المحلية ذات الشخصية المعنوية العامة .

رابعا: الشركات أو المؤسسات التي يكون للدولة أو أحد الأشخاص المعنوية العامة الأخرى ، نصيب في رأس مالها لا يقل عن 50 % منه ، أو تضمن لها حدا أدنى من الأرباح .

نبذة عن أساليب وأدوات التدقيق الالكتروني بديوان المحاسبة الكويتي

- البرامج التقليدية المستخدمة في عمليات تحليل البيانات والتحليل المالي.

  Microsoft excel – Microsoft access

- البرامج المختصة في التدقيق والخاصة بديوان المحاسبة والتي تستخدم كأداة لجمع وتحليل البيانات لمراجعة الحسابات.

  IDEA

- البرامج المستخدمة في الجهات محل التدقيق.

  ORACAL – DIMS – E-BEAMS - CITRIX

مخاطر التشغيل الإلكتروني للبيانات

أصدر ديوان المحاسبة الدليل الإرشادي لمرحلة التخطيط للتدقيق المبني على المخاطر في أكتوبر 2022 وذلك لحرص ديوان المحاسبة على مواكبة أحدث ما يطرأ من تغييرات ومن أجل تحقيق أفضل الممارسات العملية لأداء العمل الرقابي، وبما يسهم في رفع قدرات مدققي الديوان على إعداد خطط التدقيق لتحقيق رقابة فعالة على أعمال وأنشطة الجهات المشمولة بالرقابة، وذلك بتوجيه أعضاء فرق التدقيق في مرحلة التخطيط نحو الأنشطة والعمليات التي تنطوي على مخاطر عالية بالجهات المشمولة بالرقابة وترتيب أولويات التدقيق عند إعداد خطة التدقيق السنوية.

حالات عملية

- **أولا: البرامج المختصة في التدقيق والخاصة بديوان المحاسبة والتي تستخدم كأداة لجمع وتحليل البيانات لمراجعة الحسابات IDEA.**

- استكمال تقييم كفاءة وفاعلية نظم تحصيل الرسوم عن الخدمات الحكومية باستخدام الطوابع المالية الالكترونية الحكومية والدفع الالكتروني لدى الجهات الحكومية
- تحليل قاعدة البيانات المالية الخاصة بمكتب العلاج بالخارج الخاص بشركة نفط الكويت لتحديد الأهمية النسبية في إعداد خطة الفحص.

حالات عملية

- **ثانياً: البرامج المستخدمة في الجهات محل التدقيق (مؤسسة البترول الكويتية وشركاتها التابعة)**

DIMS – E-BEAMS – CITRIX – ORACAL

- استخدام برنامج DIMS كوسيلة للاطلاع على كافة المستندات والمراسلات الموجودة بالجهة المشمولة بالرقابة ومقارنتها بما يتم تزويدنا به من ذات الجهة.
- استخدام برنامج E-BEAMS كوسيلة للاطلاع على كافة البيانات والاعتمادات المالية في الجهة المشمولة بالرقابة.
- استخدام برنامج CITRIX كوسيلة لاستخدام الحاسب الالي الخاص بجهة العمل للاستفادة بكامل برامجه وخصائصه عن بعد بصورة امنة.
- استخدام برنامج ORACAL كوسيلة للاطلاع على بيانات العاملين بجهة العمل.

شكرا لحسن استماعكم،،

جمهورية مصر العربية
الجهاز المركزي للمحاسبات

التدقيق على نظم المعلومات في ظل التشغيل الإلكتروني للبيانات

تجربة الجهاز المركزي للمحاسبات

المحتويات

مقـــــــدمـــــة

- إن تغير البيئة الاقتصادية العالمية وظهور تكنولوجيا المعلومات وتغلغلها في مختلف المجالات ومن بينها مجال المجاسبة والتدقيق, كرس نوعاً من المسئوليات الجديدة أمام المحاسبين والمدققين الذين وجدوا أنفسهم أمام ضرورة التكييف مع هذه التغيرات والتطورات والتي أثرت بشكل واضح على مختلف إجراءات مهمة التدقيق.
- من هنا أصبحت عملية تدقيق نظم المعلومات أحد الموضوعات الرئيسية لعمليات التدقيق التي تجريها الأجهزة العليا للرقابة في جميع أنحاء العالم.

أهداف تدقيق نظم المعلومات

إن الهدف الأساسي من عمليات تدقيق تكنولوجيا المعلومات هو التأكيد على أن موارد تكنولوجيا المعلومات تؤدي إلى تحقيق الأهداف التنظيمية بفعالية واستخدام الموارد بكفاءة فضلاً عن :

- مراجعة ضوابط تكنولوجيا المعلومات للتأكيد على دقتها وفعاليتها.
- تقييم أداء النظام وأمنه.
- فحص عملية تطوير النظام والإجراءات المرتبطة به.

التحديات التي تواجه عمليات تدقيق نظم المعلومات

وتتمثل أهم تلك التحديات في :

- صعوبة التحقق من مصداقية البيانات المالية الإلكترونية.
- صعوبة الكشف عن التلاعب بالمعلومات المُحاسبية الإلكترونية.
- صعوبات ترتبط بنقص كفاءة مُدققي الحسابات في بيئة العمل الإلكترونية.
- صعوبة التحقق من مصدر البيانات الإلكترونية للمُعاملات المالية.
- ضعف البنية التحتية التقنية في العديد من الجهات.

تجربة الجهاز المركزي للمحاسبات

أثر التحول الرقمي على رقابة الجهاز المركزي للمحاسبات

الرقابة التي يقوم بها الجهاز في بيئة تكنولوجيا المعلومات تتضمن:

- فَهم التأثير العام لتكنولوجيا المعلومات على العمليات التجارية الرئيسية.
- فَهم كيفية تأثير استخدام تكنولوجيا المعلومات لمُعالجة المعلومات وتخزينها ونقلها والمخاطر المتأصلة ومخاطر الرقابة.
- تقييم فاعلية الضوابط على عمليات تكنولوجيا المعلومات التي تؤثر على مُعالجة المعلومات المالية في الجهات الخاضعة للرقابة.

- تقييم أداء أنظمة تكنولوجيا المعلومات المُستخدمة.
- فحص كفاءة وفاعلية عمليات إدارة نُظم المعلومات والبرامج والتقنيات.
- تقييم ما إذا كانت ضوابط تكنولوجيا المعلومات تتوافق مع القوانين والقواعد واللوائح.

استجابة الجهاز المركزي للمحاسبات للتطورات التكنولوجية

إنطلاقاً من عضوية الجهاز في لجنة الإنتوساي لتبادل المعرفة والخدمات المعرفية وعضويته بمجموعات عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات وتأثير العلم والتكنولوجيا على المراجعة والبيانات الضخمة ويشارك بفعالية في كافة الأحداث التي يتم تنظيمها في مجال العمل الرقابي.

تم توقيع الجهاز لبروتكول تعاون مع وزارة الاتصالات وتكنولجيا المعلومات التي تضمنت:

- إنشاء شبكه معلومات كاملة وتطوير قطاع الحاسب الآلي بالجهاز ودعمه بالأجهزة والتطبيقات وتراخيص التشغيل اللازمة.
- توفير البنية الأساسية لأنظمة الاتصالات اللازمة لميكنة عدد (36) ادارة لمراقبة الحسابات، وربطها مع (27) إدارة مركزية بشبكة المعلومات الرئيسية بالجهاز.
- توفير نظام الأرشفة الالكترونية بكافة إدارات الجهاز المركزي للمحاسبات.
- إنشاء تطبيقات عامة تخدم العمل الإداري داخل الجهاز، وتطبيقات رقابية تساعد العاملين في الجهاز على أداء مهامهم الرقابية.

استجابة الجهاز المركزي للمحاسبات للتطورات التكنولوجية

- تطوير البنية التحتية لغرفة التحكم المركزية وتحديث وتوفير الهارد وير والسوفت وير المشغل لها وتأمينها.
- الحصول المستمر على الاستشارات الفنية لتطوير الأعمال في مجالات تكنولوجيا المعلومات .
- إعادة هيكلة الإدارة المعنية بنُظم المعلومات والتحوّل الرقمي وتطوير اختصاصاتها وإسناد مهام إضافية لها بما يضمن سرعة الاستجابة والتغلب على التحديات ذات الصلة.
- توقيع اتفاقيات تعاون مع جهات التدريب الخارجية لتوفير التدريب وورش العمل لأعضاء الجهاز في هذا المجال.

أهم الملاحظات المكتشفة والمتكررة لأنظمة المعلومات والمخاطر المرتبطة بها

مخاطر الأمان والوصول:

- عدم تغيير كلمات المرور بصورة دورية يمكن أن يؤدي إلى وصول غير مصرح به للبيانات والموارد.
- عدم وجود سجلات مراقبة حركات المستخدمين يعيق الكشف عن الأنشطة غير المعتادة والاحتمالية لحوادث الأمان.
- استخدام كلمات مرور ضعيفة أو قصيرة أو عدم تطبيق سياسات تعقيد كلمات المرور يزيد من مخاطر الوصول غير المصرح به.
- عدم تنفيذ إجراءات تأمين متعددة العوامل لتعزيز الحماية من الوصول غير المصرح به.
- عدم تحديد مستويات الوصول وفقًا لمبدأ "أقل الامتياز" يمكن أن يزيد من تعرض النظام لمخاطر الاختراق.

أهم الملاحظات المكتشفة والمتكررة لأنظمة المعلومات والمخاطر المرتبطة بها

مخاطر إدارة المستخدمين:

- عدم وجود مراجعات دورية لصلاحيات المستخدمين يمكن أن يؤدي إلى صلاحيات غير ملائمة ومخاطر انتهاك الأمان.
- عدم وجود إجراءات تعيين وفصل وإنهاء خدمات المستخدمين يزيد من مخاطر الحسابات النشطة غير المراقبة.
- عدم تدريب المستخدمين على ممارسات الأمان يمكن أن يسهم في زيادة مخاطر الاختراق.
- تأخير في تعطيل حسابات المستخدمين بعد انتهاء خدماتهم يمكن أن يزيد من مخاطر الوصول غير المصرح به.
- عدم تحديد مسؤوليات المستخدمين بشكل واضح يمكن أن يؤدي إلى تداخل الصلاحيات وزيادة مخاطر الأمان.

أهم الملاحظات المكتشفة والمتكررة لأنظمة المعلومات والمخاطر المرتبطة بها

مخاطر البنية التحتية التقنية:

- استخدام أنظمة وبرامج وأجهزة غير مدعمة يمكن أن يؤدي إلى مشكلات توافق وأمان.
- تحديثات غير مختبرة يمكن أن تسبب مشاكل في الأمان والاستقرار.
- عدم تنفيذ إجراءات احتياطية منتظمة واختبارها يمكن أن يؤدي إلى فقدان البيانات في حالة الكوارث.
- استخدام أجهزة قديمة وغير محدثة يمكن أن يتيح الفرصة للمهاجمين للاستفادة من ثغرات معروفة.
- عدم تقديم تدريب منتظم للموظفين المسؤولين عن البنية التحتية التقنية يمكن أن يؤدي إلى قرارات غير صحيحة فيما يتعلق بالأمان والصيانة.

أهم الملاحظات المكتشفة والمتكررة لأنظمة المعلومات والمخاطر المرتبطة بها

مخاطر السجلات والمراقبة:

- عدم تفعيل ضوابط الرقابة في مراكز البيانات وعدم وجود سجلات للزائرين يمكن أن يؤدي إلى ضعف الأمان الجسدي.
- عدم وجود سجلات دقيقة لحركات المستخدمين يمكن أن يجعل من الصعب تتبع وفهم الأنشطة غير المعتادة.
- تأخر في مراجعة وتحليل سجلات الأمان يمكن أن يتسبب في عدم اكتشاف الأحداث الغير معتادة في الوقت المناسب.
- استخدام أنظمة مراقبة غير فعّالة يمكن أن يؤدي إلى تفويت أحداث هامة في عملية المراقبة.
- عدم وجود سياسات وإجراءات واضحة لمراقبة الأمان والاستجابة للحالات الأمنية يمكن أن يزيد من مخاطر فقدان البيانات والاختراق.

أمثلة لحالات الغش التي تم اكتشافها من خلال أدوات تحليل البيانات

- اصدار أوامر شراء للموردين خارج تطبيق المشتريات، ويتم سدادها من خلال العهد النقدية, حتى يمكن تخطي الإجراءات المعتمدة، وبتحليل هذه الحالات تبين شراء أصناف دون التحقق من مدي الحاجة لها والتحقق من توافرها في المستودعات والشراء تم بأسعار تزيد عن الأسعار المعتادة.
- تلاعب في معدلات الرواتب والبدلات التي يحصل عليها بعض الموظفين عن الطريق التواطؤ بين بعض الموظفين واحد مسئولي نظام شئون الموظفين، حيث تبين وجود زيادات غير طبيعية في الاستحقاقات التي يحصلون عليها.
- بمقارنة أسعار صرف العملات عند تحصيل الاستحقاقات من العملاء، تبين تسوية الفروق بين المبالغ المحصلة والمبالغ المستحقة عن طريق إعادة احتساب سعر العملة بحيث يتطابق المبلغ المحصل مع المبلغ المستحق وتسوية المتبقي في حسابات فروق العملة.

أمثلة لحالات الغش التي تم اكتشافها من خلال أدوات تحليل البيانات

- تخطي النظام الخاص بمطابقة الدفعات مع الاستحقاقات الخاص بسلف الموظفين حتى يمكن تخطي النظام الذي يقوم بخصم هذه السلف تلقائيا من حسابات الموظفين، بالإضافة الي إمكانية الحصول على سلف إضافية بالرغم من عدم سداد السلف القديمة بالمخالفة للنظام، وتبين وجود ارصدة مستحقة لموظفين قاموا بترك الخدمة دون سداد ارصدة السلف المستحقة عليهم نظرا لعدم ظهورها في نماذج ترك الخدمة.
- تخطي حدود صلاحيات المشتريات عن طريق تقسيم المعاملات حيث تبين تقسيم المشتريات التي تتجاوز حدود هذه الصلاحيات الي معاملات بمبالغ أصغر متعددة في فترات متقاربة، وذلك حتى يتمكن بعض مسئولي المشتريات من تنفيذ هذه المعاملات عن طريق الشراء المباشر دون الالتزام بالإجراءات التي تتطلب مزايدات او الحصول على عدة عروض من موردين مختلفين للحصول على أفضل الأسعار.

أمثلة لحالات الغش التي تم اكتشافها من خلال أدوات تحليل البيانات

- تبين وجود معاملات مع بعض الموردين التي تربطهم قرابة مع موظفي المشتريات من خلال مطابقة الأسماء والعناوين البريدية الحسابات البنكية وأرقام الهواتف وبعض البيانات الأخرى بين الموظفين وسجلات الموردين، بالمخالفة لساسة تضارب المصالح.

- تم استخدام تحليل البيانات لكشف التلاعب والتزوير في إشعارات رد البضاعة حيث اظهر تحليل البيانات تكرارًا غير طبيعي للأرقام المسلسلة في الإخطارات، وهو أمر غير مألوف ولا يتوافق مع القواعد المعتمدة. ثم تم تحليل عمليات الدفع وتسجيل الإشعارات وتم كشف هذا الاحتيال وحصر قيمة البضائع التي تم استلامها من قبل موزعي الشركة دون تخزينها بمخازن الشركة وبيعها بالأسواق الخارجية دون معرفة الشركة.

شكراً لكم

Kingdom of Bahrain
National Audit Office

مملكة البحرين
ديوان الرقابة المالية والإدارية

اللقاء التدريبي حول

مخاطر التشغيل الإلكتروني للبيانات وكيفية اكتشاف وسائل الغش ومواطن الفساد

الديوان العام للمحاسبة بالمملكة العربية السعودية
22 – 26 أكتوبر 2023

تقديم الموظفين
سلمان البوسميط
عبدالرحمن الهاجري
مازن محمد

المحاور الرئيسية

1. مقدمة عن ديوان الرقابة المالية والإدارية بمملكة البحرين.
2. الرقابة على نظم المعلومات في ديوان الرقابة المالية والإدارية.
3. الحالة العملية للتدقيق على نظم المعلومات.

إنشـــاء ديـــوان الرقـــابة الماليـــة والإداريـــة

تم إنشاء الديوان بموجب المرسوم بقانون رقم (16) لسنة 2002 الصادر بتاريخ 3 يوليو 2002، المعدل بالمرسوم بقانون رقم (49) لسنة 2010 الصادر بتاريخ 14 نوفمبر 2010.

يعتبر الديوان جهازاً مستقلاً مالياً وإدارياً عن السلطتين التشريعية والتنفيذية ويتبع جلالة الملك مباشرة.

أنواع الرقابة التي يمارسها الديوان

- الرقابة المالية
- رقابة الأداء
- رقابة الالتزام
- رقابة نظم المعلومات
- التدقيق الاستقصائي

قانون ديوان الرقابة المالية والإدارية

البند (ب) من المادة (6) من قانون الديوان

دراسة وفحص الأنظمة الإدارية والمحاسبية والرقابة الداخلية المتعلقة ببرامج الحاسب الآلي للتحقق من كفاءة وكفاية تلك الأنظمة وتحديد أوجه النقص والقصور فيها، والتأكد من حماية تلك الأنظمة من الاختراق، واقتراح الوسائل المناسبة لمعالجة أوجه القصور.

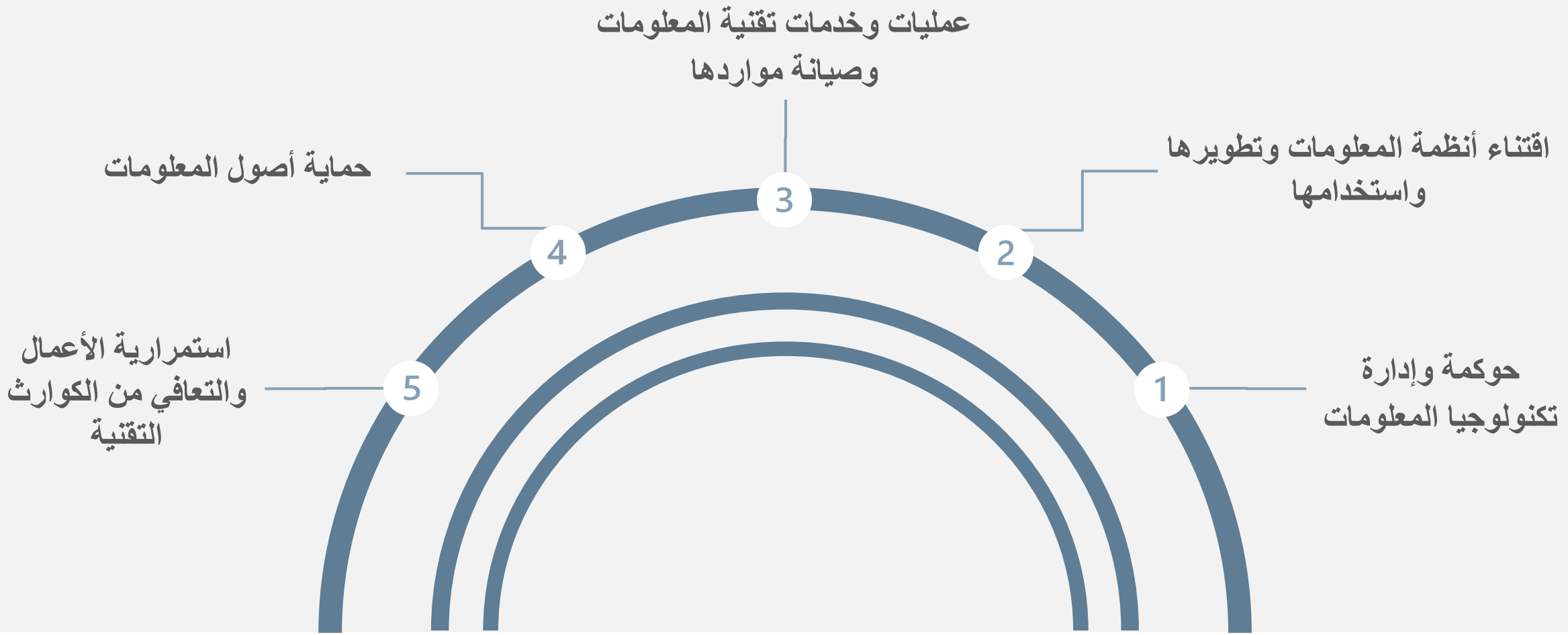
مهام رقابة نظم المعلومات في الديوان

تضمنت العديد من مهام رقابة الأداء ورقابة الالتزام التي نفذها الديوان ملاحظات حول الأنظمة الآلية الخاصة بالجهات المشمولة بالرقابة، وقد تم تقديم العديد من التوصيات الهامة لتطوير تلك الأنظمة وإحكام أنظمة الرقابة الداخلية بها.

قام الديوان منذ نشأته بعدد من المهام الرقابية على نظم المعلومات في الجهات المشمولة برقابته، وذلك من خلال التعاون مع مؤسسات التدقيق في القطاع الخاص، كلما كان هناك حاجة لمثل هذا النوع من الرقابة.

تم في سنة 2020 إنشاء وحدة متخصصة لأعمال رقابة نظم المعلومات بالديوان، وتم التوسع في ذلك حيث تم في أغسطس 2023 إنشاء إدارة لرقابة نظم المعلومات. شرع الديوان منذ السنة المهنية 2021/2020 بالتوسع في تنفيذ مهام رقابة نظم المعلومات، وذلك من خلال القيام بمهام رقابية دورية ضمن الخطط السنوية للديوان.

مجالات الرقابة على نظم المعلومات



نطاق الرقابة على نظم المعلومات

التدقيق المستقل على نظم المعلومات والذي يغطي مجالًا واحدًا أو أكثر من مجالات تدقيق نظم المعلومات الخمسة آنفة الذكر.

تدقيق متكامل ضمن مهام التدقيق المالي أو الالتزام أو الأداء لتوفير التأكيدات المتعلقة بتكنولوجيا المعلومات.

مفهوم وأهداف الرقابة على نظم المعلومات

فحص أنظمة المعلومات والموارد ذات الصلة والتحقق مما يلي:

- توافقها مع القوانين والأنظمة وتحقيقها لأهداف عمل الجهة بفاعلية
- سلامة وفاعلية تطبيق الضوابط الداخلية فيها وتقييم أداؤها
- كفاءة وفاعلية إدارة خدمات تقنية المعلومات
- تنفيذ المتطلبات الأساسية لأمن المعلومات والأمن السيبراني
- استخدام الموارد التقنية بكفاءة وفاعلية
- حماية أصول المعلومات والحفاظ على سرية ونزاهة وتوافر البيانات

أمثلة على المعايير الرقابية التي يتم الاستناد إليها

دليل مستوى الصلاحيات المعتمد للنظام الآلي

المعايير الصادرة عن المنظمة الدولية للمعايير (ISO Standards)

المهام والمسئوليات المعتمدة للإدارات والأقسام ذات العلاقة

أنظمة الرقابة الداخلية السليمة وفقاً لأفضل الممارسات في مجال استخدام تكنولوجيا المعلومات

الحالة العملية للتدقيق على نظم المعلومات

أمثلة على الإجراءات الرقابية التي يتم تنفيذها لتقييم نظم المعلومات

- التحقق من وجود ربط بين الأنظمة المستخدمة في عمليات الجهة التي يتم التدقيق عليها بأنظمة جهات أخرى لتسيير الأعمال.
- التحقق من عدم دخول أشخاص غير مصرح لهم على النظام الآلي.
- التحقق من وجود توثيق مكتمل لمراحل إعداد وتطوير الأنظمة المستخدمة بالجهة، بما يمكن من الرجوع إليها عند عمليات التطوير أو التغيير اللاحقة على الأنظمة.
- التحقق من وجود خاصية تتبع أثر العمليات المنجزة في الأنظمة الآلية.
- التحقق من وجود خطط لدى الجهة التي يتم التدقيق عليها تتعلق باستمرارية العمل والاستجابة للحوادث التقنية وللتعافي من الكوارث التقنية الخاصة باستعادة الأنظمة التطبيقية وبياناتها خلال حالات التعطل عند تعرضها للحوادث والكوارث التقنية والأمنية.

شكراً على حسن استماعكم

لقاء تدريبي حول « مخاطر التشغيل الالكتروني
وكيفية اكتشاف وسائل الغش ومواطن الفساد
من 22 الى 26 أكتوبر2023
المملكة العربية السعودية

تجربة مجلس المحاسبة الجزائري بخصوص مخاطر التشغيل الإلكتروني للبيانات وكيفية اكتشاف وسائل الغش ومواطن الفساد

من إعداد :
الأستاذ : مولود بركاتي
الأستاذة : فيروز بن رحاب
الأستاذ : حميد أفقير

محاور المداخلة

1. جلس المحاسبة الجزائري
2. التشغيل الالكتروني للبيانات المحاسبية وقواعد ضبطه في الجزائر
3. الحالة العملية: تقييم نظام المعلومات للمؤسسة العمومية لي رحموني

1- تقديم مجلـــس المحاسبـة

أنشئ مجلس المحاسبة بموجب المادة 190 من دستور 1976 وقد عرف التعديل الدستوري لسنة 2020 في مادته 199 مجلس المحاسبة بأنه مؤسسة عليا مستقلة للرقابة على الممتلكات والأموال العمومية. يكلف بالرقابة البعدية على أموال الدولة والجماعات المحلية والمرافق العمومية وكذلك رؤوس الأموال التجارية التابعة للدولة، كما يساهم في ترقية الحكم الراشد والشفافية في تسيير الأموال العمومية وإيداع الحسابات.

2- التشغيل الالكتروني للبيانات المحاسبية وقواعد ضبطه في الجزائر

مقدمة: يعتبر تشغيل البيانات الكترونيا ضمن نظام المعلومات مصدرا رئيسيا للمعلومات في أي مؤسسة، حيث تعتمد عليه الإدارة لتوفير المعلومات اللازمة وفي الوقت المحدد، لذا تسعى كل المؤسسات لتطوير وتحديث هذا النظام باستمرار من خلال استخدام تكنولوجيا المعلومات التي توفر الدقة، السرعة، وتخفض التكلفة .

الأمرالذي أدى الى تغير عملية معالجة البيانات وتخزينها، مما يستوجب تطوير الضوابط الرقابية.

وأمام كل هذا، فإن التدقيق في ظل بيئة التشغيل الإلكتروني يستوجب من المدقق دراسة وفهما جيدا للبيئة االتي تتم فيها معالجة البيانات حتى يسهل فهم النظام المحاسبي ونظام الرقابة الداخلي للمؤسسة، الأمرالذي يتطلب استخدام أساليب وإجراءات حديثة والاستفادة من مزايا تكنولوجيا المعلومات .

مفهوم التشغيل الإلكتروني للبيانات:

يعرف بأنه النظام الذي يعالج البيانات على اختلاف أنواعها (بيانات محاسبية، بيانات مالية) معالجة الكترونية وهذا عن طريق الحاسوب .

ويتشكل نظام التشغيل الإلكتروني من مجموعة الأجهزة والبرامج الإلكترونية التي يتم استخدامها في تخزين البيانات وتحويلها إلى معلومات لحين استخدامها بواسطة المستخدمين في اتخاذ القرارات ومزاولة الأنشطة، ويتكون نظام التشغيل الإلكتروني من مجموعتين أساسيتين من العناصر المادية و البرامج، تتمثل العناصر المادية في مجموعة الأجهزة اللازمة لإدخال البيانات إلى الحاسوب وتشغيلها وتلقي المعلومات بينما تتمثل البرامج في مجموعة الأوامر اللازمة لتشغيل الحاسوب وكذلك معالجة البيانات

معايير التدقيق في ظل بيئة نظم المعلومات الإلكترونية

معيار التدقيق الدولي (ISA401) :

يعتبر المعيار401(التدقيق في ظل بيئة نظم االمعلومات الإلكترونية)هو المعيار الرئيسي االمرتبط بتكنولوجيا المعلومات.

1- **هدف المعيار** :يهدف هذا المعيار الى توفير الإجراءات التي يجب إتباعها عند تنفيذ عملية التدقيقعلى المؤسسة ذات التشغيل الإلكتروني لبياناتها المالية.

2- **الكفاءات والمهارات المطلوبة من المدقق** :يجب أن يكون المدققعلى معرفة بالحسابات وذلك للتخطيط والإدارة والإشراف والفحص، كما يجب أن يكون متمكنا من استخدام الحاسب في تنفيذ بعض إجراءات التدقيق، وقد يستعين المدقق بالخبير من الخارج بحيث يكون له معرفة بالحاسبات.

3 - مبادئ المعيار الدولي 401:

يجب على المدقق المراجع :

- أن يحدد نظم االمعلومات الإلكترونية على عملية التدقيق.
- أن تكون لديه المعرفة التامة بنظم المعلومات الإلكترونية وذلك لتخطيط ومراقبة وفحص العمل المنفذ .
- أن يحدد إمكانية الاستعانة بخبير ذو مهارات في نظم المعلومات الإلكترونية عند تنفيذ عملية التدقيق.
- الحصول على أدلة التدقيق الكافية والملائمة عند الاستعانة بالخبير خلال مرحلة التخطيط.
- الحصول على الفهم الكامل عن أنشطة نظم المعلومات الإلكترونية والتحقق من مدى توافر البيانات لاستخدامها في عملية التدقيق.
- الحصول على الفهم الكاف لبيئة نظم المعلومات الإلكترونية والتحقق من تأثير البيئة على تقييم المراجع للمخاطر الحتمية و مخاطر الرقابة .
- تصميم إجراءات التدقيق بالاعتماد على نظم المعلومات الإلكترونية وذلك لتخفيض خطر التدقيق الى أدنى مستوى القبول.

قواعد ضبط المعالجة الآلية للبيانات المحاسبية في الجزائر

لقد تم ضبط عملية المعالجة الآلية للبيانات المحاسبية في الجزائر وذلك من خلال المرسوم التنفيذي رقم 09 - 110 المؤرخ في 11 ربيع الثاني عام 1430 الموافق 7 أبريل سنة 2009 الذي يحدد شروط وكيفيات مسك المحاسبة بواسطة أنظمة الإعلام الآلي حيث تم تحديد مجموعة من أنظمة الإعلام الآلي وكذا الخصائص و المعايير الواجب توفرها في البرامج التطبيقية المحاسبية.

شروط مسك المحاسبة آليا حسب المرسوم التنفيذي رقم 09 - 110

- ✓وجوب توفر مستلزمات المعالجة الآلية (معدات، برامج).
- ✓ وجوب الالتزام بالمبادئ المحاسبية المعمول بها.
- ✓ وجوب توفر مستندات الإثبات.
- ✓ تعريف إصدارات نظام الإعلام الآلي و يجب أن ترقم وتؤرخ.
- ✓وجوب تطبيق طابع عدم التشطيب أو تصحيح التسجيل.
- ✓وجوب إعداد ملف يبين الإجراءات و التنظيم المحاسبي، بشكل يسمح بفهم نظام المعالجة ومراقبته ويحفظ هذا الملف مع كل التحيينات التي تطرأ لمدة توافق تلك التي يتطلبها عرض الوثائق المحاسبية التي يستند عليها

- ✓وجوب اصدار تعهد من طرف معد البرنامج المعلوماتي ينص على مطابقة البرنامج المعلوماتي للتعليمات المقررة في المرسوم.
- ✓وجوب حفظ لمعطيات آليا في حالة المعالجة اليدوية التي تؤدي الى خطر فقدان أو فساد المعطيات.

المعايير الواجب توفرها في البرامج التطبيقية المحاسبية وآليات الرقابة حسب المرسوم التنفيذي رقم 09 - 110

- ✓ يجب أن يحتوي البرنامج المعلوماتي للمحاسبة المستعمل على ملف يصف الشكل والخاصيات التي يمكن طبعها أو توفرها على شكل إلكتروني .أي الوظائف التي يقوم بها.
- ✓ يجب على النظام المعلوماتي منع أي تعديل أو حذف لأي عملية بعد التصديق على التسجيلات المحاسبية؛
- ✓يجب إعداد كل الكشوف التي يجب على المؤسسة إعدادها طبقا للأحكام القانونية
- ✓ يجب إحترام مبدأ القيد المزدوج.

- ✓ يجب على النظام المعلوماتي منع أي تعديل أو حذف لأي عملية بعد التصديق على التسجيلات المحاسبية.
- ✓ يجب التذكير بالتصديق على مجموع التسجيلات المسجلة قبل إقفال كل سنة مالية
- ✓ يجب أن يحتوي البرنامج المعلوماتي على إجراء يسمح بفتح الميزانية آليا و التي يجب أن تكون مطابق للميزانية الختامية.
- ✓ يجب أن يحتوي البرنامج المعلوماتي على وظيفة تمكن من إرسال بطاقة التسجيلات للغير وبشكل قابل للاستغلال بسهولة وبمعزل عن البرنامج المعلوماتي
- ✓ يجب أن يحفظ البرنامج المعلوماتي أثر تحديثه في بطاقة تظهر التحديثات ومحتواها على التوالي تسمى اليومية.

- ✓ يجب أن تظهر الكشوف التي يتم إعدادها بواسطة البرنامج المعلوماتي كل المعلومات الواجب توفرها في هذه الكشوف
- ✓ يجب أن يتضمن البرنامج المعلوماتي مقاييس الرقابة والأمن التي تمنع أي إستغلال من طرف الأشخاص غير المرخص لهم
- ✓ يجب أن يتضمن البرنامج المعلوماتي إجراء للأرشيف ويسمح بنقل المعطيات نحو دعائم التخزين القابلة للنقل دون إمكانية التعديل
- ✓ يجب أن يحتوي البرنامج المعلوماتي للمحاسبة إجراء يسمح بحفظ كل البطاقات الضرورية من أجل القيام بإصلاح كامل للنظام المحاسبي أو يكون مرجعا لإجراء الإصلاح و الحفظ.

3- الحالة العملية

تقييم نظام المعلوماتSI للمؤسسة العمومية الاستشفائية جيلالي رحموني

محاور الحالة العملية

1- تقديم مهمة الرقابة؛
2- اعداد مصفوفة المخاطر ؛
3- نتائج عملية المراجعة ؛
4- التوصيات.

1- تقديم مهمة الرقابة

في إطار تنفيذ البرنامج الرقابي السنوي لسنة 2018 ، قام مجلس المحاسبة الجزائري بإجراء عملية رقابة الأداء للمؤسسة العمومية الاستشفائية جيلالي رحموني .

حيث تمحورت عملية الرقابة على تقييم شروط تسيير الموارد البشرية والمالية والمادية فضلا عن مستوى التكفل بمهام المؤسسة. وضمن هذا السياق تم تقييم النظام المعلوماتي للمؤسسة

المؤسسة العمومية الاستشفائية جيلالي رحموني ، هي مؤسسة صحية عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلال المال، وهي تحت وصاية الوالي وتغطي (9) بلديات بعدد ساكنة يقدر بـ 700000 نسمة.

النظام المعلوماتي SG الخاص بالمؤسسة

يتشكل النظام المعلوماتي الموضوع على مستوى المؤسسة الاستشفائية من ستة وثمانين (86) حاسوبا و خوادم اثنين (02) SERVEUR، وأربعة عشر (14) مخزن كهرباء onduleurs و ستة وسبعين (76) طابعة، إضافة الى خمسة وعشرين جهاز تصوير طبق الأصل و جهاز ماسح ضوئي scanner، و جهاز تضمين (MODEM) زائد خزانة مزج armoire de brassage ومجموعة من التطبيقات.

فيما يتعلق بالتطبيقات، يحتوي النظام المعلوماتي للمؤسسة العمومية الاستشفائية على ثمان (8) تطبيقات حاسوبية، مفصلة في الجدول أدناه:

الرقم	التعيين	الوظيفة	المصلحة المستخدمة
1	EPIPHARME	تسيير الأدوية	مصلحة الصيدلة
2	PATIENT	ادخال بيانات المرضى المتعالجين في المؤسسة	المديرية الفرعية لمصالح الصحة
3	GARDE	تسيير المناوبة	المديرية الفرعية لمصالح الصحة
4	DHIS	حساب أنشطة الصحة	المديرية الفرعية لمصالح الصحة
5	SISDZ	الأمراض والتصريحات الالزامية	مصلحة الأوبئة
6	WPAYE	تسيير الأجور	المديرية الفرعية للمالية والوسائل
7	SIRH	تسيير ملفات الموظفين	المديرية الفرعية للموارد البشرية
8	TRICOH	محاسبة المستشفيات الثلاثية	مكتب الاعلام الالي

2- اعداد مصفوفة مخاطر تشغيل البيانات الكترونيا

أهم المخاطر المتعلقة بتشغيل البيانات الكترونيا على مستوى المؤسسة والتي حددتها فرقة الرقابة تتمثل في:

مخاطر متوقعة بسبب أخطاء تقنية

مخاطر حفظ البيانات والمعلومات

مخاطر بسبب الأخطاء البشرية والبيئية

على التفصيل التالي:

مخاطر تقنية

1. خطر الاختراق.
2. خطر الفيروسات.
3. خطر الُّدخول غير الُمصرَّح به.
4. خطر استخدام الُّنسخ غير الأصلّية من البرامج.
5. خطر التّعديل غير المصرَّح به للبيانات أو المعلومات.
6. خطر دّقة البيانات والمعلومات وتوافقها وتكاملها.
7. خطر أعطال الأجهزة أو البرامج.

مخاطر بشرية

1. خطر نقص المهارات والكفاءات.
2. خطر الأخطاء البشرية.
3. خطر سرقة الخوادم وأجهزة التخزين.

مخاطر بيئية ومخاطر بيئة العمل

1. خطر فقد البيانات بسبب الكوارث الطبيعية(الفيضانات، الحرائق، الّزلازل).
2. خطر انقطاع التّيار الكهربائي.
3. خطر انقطاع الدعم الفني والصيانة من مزودي الخدمات لمركز الحاسوب.

بعد تحديد أهم المخاطر الممكنة، قامت فرقة الرقابة لمجلس المحاسبة ببناء مصفوفة المخاطر على النحو التالي:

مصفوفة المخاطر

تأثير الخطأ عند حدوثه ⇦ احتمال حدوث الخطر ⇩	شديد الخطورة 5	خطير 4	متوسط 3	منخفض 2	منخفض جدا 1
عالي جدا 5	25	20	15	10	5
عالي 4	20	16	12	8	4
متوسط 3	15	12	9	6	3
منخفض 2	10	8	6	4	2
منخفض جدا" 1	5	4	3	2	1

تحديد الخطر	وصف الخطر	احتمال وقوع الخطأ من 1 إلى 5 (أ)	الأثر المحتمل من 1 إلى 5 (ب)	تقييم الخطر من 1 إلى 25 من خلال ضرب (أ) في (ب)
خطر الفيروسات	وهي برامج إذا ما اخترقت الخوادم ربما تسبب دمار أو فقد للبيانات او المعلومات أو غيرها من الأضرار التي تسببها الفيروسات	4	4	16
أعطال الأجهزة والبرامج	يتمثّل هذا الخطر في تعُّطل الأجهزة الرئيسة للمؤسسة، أو البرامج والأنظمة التي تعنى بتسيير أهّم العملّيات أو الخدمات التي تقّدمها المؤسسة.	4	4	16
نقص المهارات والكفاءات	يتمثّل هذا الخطر في عدم توافر الكفاءات والمها ارت الخاصة بتقنية معالجة المعلومات والبيانات الكترونيا.	4	4	16

عدم التناسق والتكامل بين مختلف البرامج والتطبيقات	انعدام التكامل والتناسق بين مختلف البرامج والتطبيقات المدمجة في النظام المعلوماتي للمؤسسة مما قد ينتج عنه تضارب في البيانات أو عدم تكاملها.	4	4	16
عدم دقة البيانات	عدم اتاحة البرامج لتسجيل جميع البيانات والمعطيات والوثائق الثبوتية، مما قد ينتج عنه معلومات خاطئة أو غير مكتملة وعدم اكتشاف الأخطاء والمخالفات والتلاعبات	4	4	16

استخدام النسخ غير الأصلية من البرامج	استخدام نسخ غير مرخصة من البرامج أو الأنظمة التي تخدم العمل، ما قد يُسبِّب التوُّقف في لحظة ما خلال العمل، أو عدم المقدرة على إجراء أعمال على تلك البرامج، بسبب توُّقفها لأنها غيرمرَّخصة.	3	4	12
خطر سرقة الخوادم وأجهزة التخزين	فُقد البيانات والمعلومات في حال سرقة الخوادم من مراكز البيانات.	3	4	12
أخطاء بشرية	يتمثّل هذا الخطر في حدوث أخطاء بشرّية غير متعّمدة أثناء ادخال وتشغيل البيانات بما يؤثر في أداء الأجهزة أو الأنظمة والتطبيقات.	3	4	12

مخاطر تقنية الاختراق (Hacking)	الدخول الجبرّي وكسر الحواجز والُجُدر النارّية الواقية للخوادم والأجهزة التي تخدم البرامج والأنظمة	2	5	10
خطر فقد المعلومات بسبب الفيضانات أو الحرائق أو الزلازل	يتمثّل هذا الخطر في فُقد البيانات والمعلومات بسبب الفيضانات أو الحرائق أو الزلازل التي تسبب في تدمير مركز المعلومات والأجهزة الخادمة الموجودة فيه التي تحتوي البيانات والمعلومات الخاصة بمختلف مصالح المؤسسة الاستشفائية	2	4	8

خطر الدخول والتعديل غير المصرح به للبيانات	الّدخول بطريقة غير ُمصرّح بها إلى الأنظمة أو البرامج أو قواعد البيانات، وذلك عن طريق الحصول على اسم المستخِدم أو كلمة الِّسر بطريقة غير مشروعة، بغية تعديل البيانات .	1	4	4
خطر انقطاع التيار الكهربائي	يتمثّل هذا الخطر في انقطاع الكهرباء عن مركز البيانات ومن ثَّم تعطلُ الأجهزة المختلفة التي تقوم بتسيير ومعالجة بيانات مختلف مصالح المؤسسة الاستشفائية	1	4	4
خطر انقطاع الدعم الفني والصيانة من المورد	يتمثّل هذا الخطر في التوُّقف المفاجئ للّدعم الفني والصيانة للأجهزة أو البرامج والتطبيقات المشتغلة	2	2	4

3- نتائج عملية الرقابة

كشفت عملية تدقيق ومراجعة النظام المعلوماتي الخاص بالمؤسسة العمومية الاستشفائية عن العديد من أوجه القصور والاختلالات، منها ما يخص حالة المعدات وشبكات الحاسوب الموجودة من جهة ،ومنها ما يتعلق بالتكامل والتناسق بين مختلف التطبيقات المستخدمة من جهة أخرى، بالإضافة الى تسجيل نقص في مؤهلات الموارد البشرية الساهرة على تشغيل النظام المعلوماتي.

بخصوص خطر أعطال الأجهزة والبرامج (وهو خطر مرتفع حسب مصفوفة المخاطر)

1- وجود تطبيقات خارج الخدمة

كشفت عملية التدقيق أن اثنان (2) *من أهم التطبيقات الموجودة على مستوى المؤسسة الاستشفائية خارج نطاق الخدمة*، ويتعلق الأمر بكل من :

- تطبيق TRICOH المتعلق بمحاسبة المستشفيات الثلاثي(محاسبة عامة ، محاسبة تحليلية ومحاسبة الموازنات) الموضوع تحت تصرف مكتب الاعلام الآلي، المنصوص عليه بالمرسوم التنفيذي رقم 14-106 الصادر في 10 جمادى الأولى 1435 الموافق 12 مارس 2014، حيث أن بعض المعدات المخصصة لها لا تعمل والبعض الآخر يستخدم في مصالح أخرى؛
- تطبيق DHIS المتعلق بحساب أنشطة الصحة الموضوع تحت تصرف المديرية الفرعية لمصالح الصحة.

2- أعطاب في التجهيزات وانعدام عملية الصيانة
وجود كمية كبيرة من معدات الاعلام الآلي بها أعطاب. وهي مكدسة عشوائيا على مستوى المديرية الفرعية للمالية والوسائل دون القيام بعملية التصليح والصيانة.

3- الخادم (السرفر) المتعلق بتطبيق patient «المريض»، المستخدم من طرف مكتب القبول لا يشتغل منذ أكثر من عامين. ولم تتخذ إدارة المؤسسة الاستشفائية أي إجراء لإصلاحه، نتيجة لذلك فإن بيانات المرضى الداخليين الى المؤسسة الاستشفائية المدخلة في هذا التطبيق يتم حفضها في القرص الصلب لجهاز حاسوب بسعة تخزين محدودة معرض لخطورة العطب في أي وقت، وهذا يزيد من خطر فقدان بعض المعلومات.

بخصوص خطر عدم التناسق والتكامل بين مختلف البرامج والتطبيقات المدمجة في نظام المعلومات (وهو خطر مرتفع حسب مصفوفة المخاطر)

ـ التطبيقات الحاسوبية المستخدمة على مستوى المؤسسة الاستشفائية منفصلة عن بعضها البعض، ولم يتم تصميمها ضمن سياق تسيير مدمج للمعلومات الاستشفائية. على سبيل المثال، تقوم المديرية الفرعية للخدمات الصحية بتشغيل ثلاثة تطبيقات حاسوبية دون أي صلة بينها. ويتعلق الأمر بالتطبيق المسمى "المريض" patient، والذي يعتني بجميع بيانات المريض من تاريخ القبول إلى تاريخ الخروج وكذلك الفواتير، والتطبيق الآخر "DHIS" مصمم لحساب الأنشطة الصحية و تطبيق ثالث مسخر لتسيير المناوبة.

بخصوص خطر عدم اتاحة البرامج تسجيل جميع البيانات والمعطيات والوثائق الثبوتية (وهو خطر مرتفع حسب مصفوفة المخاطر)

عدم اتاحة التطبيقات المستعملة على مستوى النظام المعلوماتي للمؤسسة تسجيل وعرض جميع البيانات والمعطيات المحاسبية والوثائق الثبوتية.

بالمقابل نجد أن التدقيق اليدوي في مختلف السجلات والعقود وحوالات الدفع والفواتير الممسوكة على مستوى المؤسسة العمومية الاستشفائية يكشف العديد من التجاوزات التي لا تظهرها هذه التطبيقات، فعلى سبيل المثال لا الحصر نجد:

- ✓ التسديد المزدوج لبعض الفواتير؛
- ✓ الحسم غير القانوني للنفقات ؛
- ✓ عدم تطبيق عقوبة التأخير على المتعاملين الاقتصاديين المتأخرين في توريد مشتريات المؤسسة أو المتأخرين في تسليم أشغال الإنجاز والصيانة.

بخصوص خطر نقص الكفاءات والمهارات (وهو خطر مرتفع حسب مصفوفة المخاطر)

سجلت فرقة الرقابة :

- عدم كفاية الموارد البشرية المسخرة لتشغيل النظام المعلوماتي للمؤسسة؛
- نقص في الكفاءات والمهارات التقنية للمشتغلين على مختلف التطبيقات المتعلقة بالنظام المعلوماتي؛
- انعدام التدريب والتكوين المستمر في مجال المعلوماتية للكوادر والمستخدمين.

4 ـ التوصيات

1. العمل على صيانة النظام المعلوماتي وسيره الحسن على المستوى المادي والبرمجي والبشري؛
2. احترام الإجراءات التنظيمية والتقنية المتعلقة بالنظام المعلوماتي للمؤسسة.

شكرا على حسن الاصغاء والمتابعة

مخاطر التشغيل الالكتروني للبيانات و كيفية اكتشاف وسائل الغش و مواطن الفساد .

فهرس المحتويات :

مخاطر التشغيل الالكتروني للبيانات و كيفية اكتشاف وسائل الغش و مواطن الفساد :

المقدمة :

تلعب أنظمة المحاسبة المحوسبة دوراً هاما في تشغيل ومعالجة وتخزين ونقل واستخلاص البيانات والمعلومات المالية لصالح المنظمة من خلال الحواسيب ووسائل الاتصال وشبكات الربط وغيرها من المعدات .

إن الأنظمة المحوسبة لها فوائد عديدة. على سبيل المثال، فإنها تقلل من الأخطاء البشرية المرتبطة بالضوابط اليدوية، وتوفر الوقت للشركات والحكومات وتسمح بالوصول السهل إلى البيانات. ومن ناحية أخرى، لديها عيوب أيضاً مثل ندرة الخبرات احياناً في بعض هذه الأنظمة خاصةً المتقدمة منها وذات لغات البرمجة المعقدة ، وإمكانية اختراق هذه الأنظمة من خلال أصحاب الخبرات واجراء العمليات المالية دون تتبع ورصد لهذه الحركات اولاً بأول .

بعض حالات الغش والاحتيال المالي المرتبط بالتشغيل الالكتروني للبيانات :

1- الوصول غير المصرح به .

2- السداد الوهمي .

3- الفاتورة الوهمية .

4- الحساب الاحتيالي .

سيتم استعراض تالياً الحالة العملية الاولى :

- قيام المدير المالي في احدى الدوائر الحكومية بتجميل الحساب الختامي من خلال القيام بعملية تضخيم مبلغ الإيرادات وذلك من خلال وجود صلاحية له حصراً على النظام المحاسبي الالكتروني بالتحكم بالمبلغ الإجمالي للإيرادات والنفقات وغيرها من الحسابات .

- وعند الرجوع الى المبالغ الافرادية للمعاملات تبين بان المبالغ الافرادية بمجموعها لا تتساوى مع المبلغ الإجمالي .

- ومن خلال الحفاظ على مبدأ الشك في التدقيق تبين ان هناك تباين عند القيام بعملية التحليل المالي بين كل من السنة السابقة والحالية بين مبالغ الإيرادات ، كما أظهرت المبالغ الموردة الى البنك عند القيام بطلب كشف حساب اختلاف بين سجلات الدائرة والبنك .

- وهو ما كان بالإمكان كشفه فيما لو كان النظام يدوي بحيث ان عمليات التحريف والشطب تكون اكثر وضوحاً من خلال المقارنة والتجميع اليومي للعمليات .

- كان هدف المدير المالي هو القيام بتوقيع عقد العمل الخاص به لسنة قادمة من خلال اظهار نتائج مخالفة للواقع ولا تعكس الحقيقة وبيان فاعلية وكفاءة سياسة التحصيل ، وذلك لحين الانتهاء من إجراءات تجديد العقد .

- إن من قام بتصميم البرنامج ليس متخصصاً بعلم المحاسبة ولم يتم تزويده او اعلامه بان تلك الصلاحية لا يجب ان تعطى لاي كان بمن فيهم المدير المالي او المدير العام .

الحالة العملية الثانية :

عند تدقيق النظام المحاسبي لإحدى الدوائر الحكومية تبين بأن النظام المحاسبي لا يقوم بتثبيت رقم مستند الصرف الملغي بل يتم استبدال الرقم الملغي بآخر صحيح بحيث أن عملية الإلغاء غير ظاهرة وكما سنبين في الشريحة التالية :

حساب البنك في النظام المحاسبي كما يجب أن يكون والذي يبين حركات القبض والصرف كما في الشكل التالي :

نوع المستند	رقم المستند	حالة المستند
مستند صرف الرواتب	502	اكتمال وتم التنفيذ
مستند صرف الاجور	503	مستند ملغي
مستند صرف الضمان الاجتماعي	504	اكتمال وتم التنفيذ
مستند صرف النثريات	505	اكتمال وتم التنفيذ
مستند صرف ضريبة الدخل	506	اكتمال وتم التنفيذ
مستند صرف العلاوات والمكافات	507	اكتمال وتم التنفيذ

- الا ان الحساب ظهر في النظام المحاسبي كما في الشكل التالي :

نوع المستند	رقم المستند	حالة المستند
مستند صرف الرواتب	502	اكتمال وتم التنفيذ
مستند صرف الضمان الاجتماعي	503	اكتمال وتم التنفيذ
مستند صرف النثريات	504	اكتمال وتم التنفيذ
مستند صرف ضريبة الدخل	505	اكتمال وتم التنفيذ
مستند صرف العلاوات والمكافات	506	اكتمال وتم التنفيذ

ما هو الخطر في مثل هذه الحالة :

- عند القيام بعملية الإلغاء الالكترونية فأن عملية الإلغاء قد تمت الكترونياً مع العلم بأن مستند الصرف الملغي قد تم طباعته وتمت عملية السير بإجراءات اعتماده وتوقيعه من صاحب الصلاحية وتسليم الشيك لصاحب العلاقة والقيام بعملية صرفه من البنك .
- ما اثار الشك والريبة هو عدم مطابقة الحسابات عند إجراء عملية التسويات البنكية فقد ظهر أن هناك عملية صرف لمبلغ دون وجود أي اثر لعملية صرف تمت في الدائرة .
- تمت مخاطبة الجهات ذات العلاقة والقيام بعملية تصحيح لخطأ النظام المحاسبي حسب الأصول .

الخاتمة :

- يسعى ديوان المحاسبة الأردني الى رفد موظفيه ومدققيه بكافة الإمكانات المتاحة وخاصةً في عصر التكنولوجيا الحديثة والتطورات التي شهدها العالم بأسره وتنوع أساليب الاحتيال والغش والفساد المرتبط بهذه التكنولوجيا لذلك وجب مواكبة هذه التطورات ورفد كافة المدققين بالأساليب الحديثة في التدقيق والدورات المتخصصة بتدقيق الأنظمة المحاسبية وغيرها ، وذلك تحقيقاً لرسالة الديوان المتمثلة بتحقيق رقابة فعالة على المال العام وفقاً لأفضل الممارسات الرقابية والمعايير المهنية .


THANK YOU
Any Questions?